

(10) 日本特許庁 (J P)

(12) 特 許 公 報 (B 1)

(11) 特許番号

特許第3445986号
(P3445986)

(45) 発行日 平成15年9月16日 (2003.9.16)

(24) 登録日 平成15年6月27日 (2003.6.27)

(51) Int. Cl. ⁷	国際分類	P I
H 0 4 L 12/06		H 0 4 L 12/06
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00
H 0 4 L 12/06		H 0 4 L 12/06
		A
		3 5 1 Z
		B

請求項の数26 (全 10 頁)

(21) 出願番号	特願2002-283287(P2002-283287)	(73) 特許権者	040605521 松下電産産業株式会社 大阪府門田大字門田1006番地
(22) 出願日	平成14年9月27日 (2002.9.27)	(72) 発明者	武嶋 秀明 大阪府門田大字門田1006番地 松下電産産業株式会社内
特許請求日	平成15年3月25日 (2003.3.25)	(72) 発明者	加藤 尚徳 大阪府門田大字門田1006番地 松下電産産業株式会社内
早期審査対象出願		(72) 発明者	武嶋 秀明 大阪府門田大字門田1006番地 松下電産産業株式会社内
		(74) 代理人	100062344 弁理士 南山 滋 (外1名)
		審査官	中木 勝

見当りに続く

64 【発明の名称】 インターネットに接続するサーバ、側面および通信システム

1

(37) 【特許請求の範囲】

【請求項1】 インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を転送する、インターネットに接続されたサーバであって、

前記機器からの定期的な通信パケットを受信し、前記端末からの前記機器に対する転送要求があった場合、前記通信パケットの応答として接続要求パケットを前記機器に送信し、

該接続要求パケットに応じて前記機器から前記サーバへ送信されたTCP接続要求を受信し、

TCP接続確立後、そのTCP接続上で前記端末と前記機器間の通信を転送することを特徴とするサーバ、

【請求項2】 前記サーバは、前記端末から機器IDを含むHTTPリクエストにより前記機器に対する転送

2

要求を受信し、

前記端末と前記機器との通信の転送を、前記端末からのHTTPリクエストを前記機器から戻られたTCP接続上に転送し、前記機器から前記TCP接続を通じて受信したHTTPレスポンスを端末へ転送することにより行うことを特徴とする請求項1記載のサーバ、

【請求項3】 前記サーバは、少なくとも1つの端末から複数の転送要求を受信することができ、前記端末から前記機器に対する複数の転送要求があった場合に、各々に対応するセッション識別子を生成して前記接続要求パケットにより機器に通知し、

前記接続要求パケットに応じて前記機器から前記サーバへ送信されたTCP接続要求を受理してTCP接続を確立し、該確立したTCP接続上で前記機器から送信されるセッション識別子を受信し、そのTCP接続に前記

特許3445988

受信したセッション識別子に対応付けることで、前記端末からの復元の接続要求に対して前記のTCP接続を各々対応付け、

前記端末がセッション識別子を指定して接続を要求し、且つ、該指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合に、前記端末からの通信をその確立済みのTCP接続上にて転送することにより、セッション識別子毎に並列して通信内容の転送を行うことを特徴とする請求項1記載のサーバ、

【請求項4】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時刻を記録する処理手段を備え、前記機器からの定期的な通知パケットを受信したときに、前記最終アクセス時刻を該受信時刻で更新し、前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が所定期間を越えている場合は該転送要求を拒否し、その差が所定期間以下の場合は該転送要求パケットの応答として接続要求パケットを前記機器に送ることを特徴とする請求項1記載のサーバ、

【請求項5】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時刻を記録する処理手段を備え、前記機器に予め最大アクセス履歴期間情報を送信し、前記機器からの定期的な通知パケットを受信したときに、最終アクセス時刻を該通知パケットの受信時刻で更新し、

前記端末から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が最大アクセス履歴期間情報に示す値を越えている場合は、前記転送要求を拒否し、その差が最大アクセス履歴期間情報に示す値以下の場合は、前記通知パケットの応答として接続要求パケットを前記機器に送ることを特徴とする請求項1記載のサーバ、

【請求項6】 前記サーバは、サーバ証明書を持ち、通信を暗号化および復号する暗号通信手段を備え、前記端末と前記機器の間で秘密情報を転送する際、予め前記端末にサーバ証明書を送信し、

前記機器により確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して暗号暗号通信手段で復号化した後、暗号暗号通信手段で暗号化して前記機器に送信し、

前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して暗号暗号通信手段で復号化した後、暗号暗号通信手段で暗号化して前記端末に送信することを特徴とする請求項1記載のサーバ、

【請求項7】 前記サーバは、サーバ証明書を持ち、通信を暗号化および復号する暗号通信手段を備え、前記端末と前記機器の間で秘密情報を転送する際、予め前記端末と前記機器に各々サーバ証明書を送信し、

前記確立されたTCP接続を介して前記端末から前記機器へ秘密情報を転送する際は、前記端末から暗号化された秘密情報を受信して暗号暗号通信手段で復号化した後、暗号暗号通信手段で暗号化して前記機器に送信し、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際は、前記機器から暗号化された秘密情報を受信して暗号暗号通信手段で復号化した後、暗号暗号通信手段で暗号化して前記端末に送信することを特徴とする請求項1記載のサーバ、

【請求項8】 インターネットに接続されたサーバと通信する、インターネットに接続された機器であって、前記サーバに定期的に通知パケットを送信し、前記サーバから接続要求パケットを受信した場合、前記サーバに対してTCP接続要求を送信し、TCP接続後、そのTCP接続上で前記サーバと通信することを特徴とする機器、

【請求項9】 前記機器は、前記TCP接続上での前記サーバとの通信を、前記サーバからHTTPリクエストを受信し、前記サーバへHTTPレスポンスを送信することにより行なうことを特徴とする請求項8記載の機器、

【請求項10】 前記機器は、Webサーバモジュールと転送モジュールを備え、

前記Webサーバモジュールは、前記転送モジュールからHTTPリクエストを受信してHTTPレスポンスを送信し、

前記転送モジュールは、前記サーバから前記接続要求パケットを受信した際は前記サーバに対してTCP接続要求を送信してTCP接続を確立し、そのTCP接続上で前記サーバからHTTPリクエストを受信して前記Webサーバに転送し、前記WebサーバからHTTPレスポンスを受信して前記サーバに前記TCP接続上で転送することを特徴とする請求項9記載の機器、

【請求項11】 前記機器は、前記サーバからセッション識別子を伴った接続要求パケットを受信した場合、前記サーバに対してTCP接続を確立し、その確立したTCP接続上で前記セッション識別子をサーバに送信し、前記TCP接続確立後は、前記TCP接続上で前記サーバと通信することを特徴とする請求項8記載の機器、

【請求項12】 前記機器は、前記サーバから最大アクセス履歴期間情報を予め受信して前記機器内に保持しておき、前記最大アクセス履歴期間情報に示す期間より短い間隔で定期的な通知パケットを送信することを特徴とする請求項8記載の機器、

【請求項13】 前記機器は、通信を暗号化および復号する暗号通信手段を備え、

前記サーバと秘密情報の送受信を確立したTCP接続上で暗号通信手段により暗号化して行なうことを特徴とする請求項8記載の機器、

【請求項14】 前記機器は、サーバ証明書を受信する

(3)

特許3445986

5

手段と通信を暗号化および復号化する暗号通信手段を備え、

前記サーバからサーバ証明書を受信し、

前記サーバと秘密情報の送受信を、前記サーバ証明書を確認して正常であることを確認した後に前記確立したTCP接続上で暗号通信手段により暗号化して行うことを特徴とする請求項8記載の機器。

【請求項15】 インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を、インターネットに接続されたサーバを介して転送する通信システムであって、前記機器は前記サーバに定期的に通信パケットを送り、前記サーバは前記端末から前記機器に対する転送要求があった場合、前記通信パケットの応答として接続要求パケットを前記機器に送り、

前記機器は、前記サーバから接続要求パケットを受信した場合、前記サーバに対してTCP接続要求を送信し、前記サーバは、前記接続要求パケットに応じて前記機器から前記サーバへ送信されたTCP接続要求を受信し、これによりTCP接続を確立し、

前記サーバは、前記TCP接続確立後、そのTCP接続上で前記端末と前記機器の間の通信を転送することを特徴とする通信システム。

【請求項16】 前記端末は前記サーバに対し機器IDを含んだHTTPリクエストを送信することにより前記機器に対する転送要求を行い、

前記サーバは前記端末と前記機器の間の通信を転送する際に、前記端末からのHTTPリクエストを前記機器から送られたTCP接続上に転送し、

前記機器は転送された前記HTTPリクエストを処理して、それに対するHTTPレスポンスを前記TCP接続上で前記サーバへ応答し、

前記サーバは前記HTTPレスポンスを端末へ転送することを特徴とする請求項15記載の通信システム。

【請求項17】 前記サーバは、少なくとも1つの端末から複数の転送要求を受信することができ、前記端末から前記機器に対する複数の転送要求があった場合に、各々に異なるセッション識別子を生成し、前記接続要求パケットにより前記機器に通知し、

前記機器は、前記サーバからセッション識別子を持った接続要求パケットを受信した場合、前記サーバに対してTCP接続を確立し、その確立したTCP接続上で前記セッション識別子をサーバに送信し、前記TCP接続確立後は、前記TCP接続上で前記サーバと通信し、

前記サーバは、前記接続要求パケットに応じて前記機器から前記サーバへ送信されたTCP接続要求を受信してTCP接続を確立し、前記TCP接続上で前記機器から送信されるセッション識別子を受信し、前記TCP接続に前記受信されたセッション識別子に対応付けるとで、前記端末からの複数の接続要求に対して複数のTCP

6

P接続を各々対応付け、

前記サーバは、前記端末からセッション識別子を指定して接続を要求し、且つ、該指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合、前記確立済みのTCP接続上で前記端末からの通信を転送することにより、セッション識別子毎に並列して通信内容の転送を行うことを特徴とする請求項15記載の通信システム。

【請求項18】 前記サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記憶手段を備え、前記サーバは、前記機器に予め最大アクセス履歴期間情報を送信し、

前記機器は、その最大アクセス履歴期間情報を受信して内部に保存しておき、前記最大アクセス履歴期間情報が示す範囲よりも短い間隔で定期的に通信パケットを送信し、

前記サーバは、前記機器から通信パケットを受信した後に最終アクセス時刻を通信パケットの受信時刻で更新し、

前記サーバは、前記機器から前記機器に対する転送要求があった際に、前記機器の最終アクセス時刻と現在時刻との差が最大アクセス履歴期間情報で示す範囲を超えている場合は前記接続要求を拒否し、その差が最大アクセス履歴期間情報で示す範囲以下の場合には、前記通信パケットの応答として接続要求パケットを前記機器に送信することを特徴とする請求項15記載の通信システム。

【請求項19】 前記サーバは、サーバ証明書を持し、通信を暗号化および復号化する暗号通信手段を備え、

前記端末は、サーバ証明書を確認する手段と通信を暗号化および復号化する暗号通信手段とを備え、

前記機器は、通信を暗号化および復号化する暗号通信手段を備え、

前記サーバは、前記端末と前記機器の間に秘密情報を転送する際、予め前記端末にサーバ証明書を送信し、

前記端末は、前記サーバと秘密情報の送受信を、前記サーバ証明書を確認して正常であることを確認した後に暗号通信手段により暗号化して行い、

前記機器は、前記サーバと秘密情報の送受信を、前記確立されたTCP接続で暗号通信手段により暗号化して行い、

前記サーバは、前記確立されたTCP接続を介して前記機器から前記機器へ秘密情報を転送する際に、前記端末から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記機器に送信し、

前記サーバは、前記機器により確立されたTCP接続を介して前記機器から前記端末へ秘密情報を転送する際に、前記機器から暗号化された秘密情報を受信して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号化して前記暗号通信手段で復号化した後、前記暗号通信手段で暗号

(5)

特許 3445986

上の機器から所望のタイミングでルータを介してローカルエリアネットワーク内の機器に対する通信を開始できる通信システムに関する。

【0002】

【従来の技術】 近年、企業、家庭を問わず、Network Address Translation機能（以下「NAT」と称す。）またはNetwork Address Port Translation機能（以下「NAPT」と称す。）を有するルータによりローカルエリアネットワーク（以下「LAN」と称す。）とインターネットとを接続することが一般化している。

【0003】 インターネットに接続された機器間で通信を行なう場合、世界中で一斉に割り当てられたグローバルIPアドレスが使用される。一方で、インターネットに接続された機器の台数によりグローバルIPアドレスは不足する傾向にある。そのため、インターネットに直接接続された機器内や家庭内のLANにおいては、RFC1918に規定されたLAN内での一連のプライベートIPアドレスが使用されることが多い。プライベートIPアドレスはインターネットにおいて一時的なアドレスでないため、そのままではプライベートIPアドレスを持つ機器はインターネットに接続された機器と通信を行うことができない。NATまたはNAPT機能はこれらの問題を解決し、プライベートIPアドレスを割り当てられた機器がインターネット経由で通信を行なえるよう、グローバルIPアドレスとプライベートIPアドレスの相互変換機能を提供する。

【0004】 以下で、NAT機能の仕組みを図8の通信シーケンス図に沿って説明する。LAN711はルータ703を介してインターネット712に接続されている。機器701はLAN711に接続され、サーバ702はインターネット712に接続されている。機器701のIPアドレスはプライベートIPアドレス「192.168.1.2」であり、サーバ702のIPアドレスはグローバルIPアドレス「4.17.168.6」であるとする。ルータ703のインターネット側IPアドレスはグローバルIPアドレス「202.224.159.14」であるとする。ルータ703のインターネット側IPアドレスは図8の便直上1つしかないとする。

【0005】 上記ネットワーク構成において、機器701がサーバ702と通信を開始するためには、機器701は、まずIPパケット704をLAN711に送出する。IPパケット704には送信元先を特定するために、ソースIPアドレス（以下「SA」と称す。）、デスティネーションIPアドレス（以下「DA」と称す。）、ソースポート（以下「SP」と称す。）、デスティネーションポート（以下「DP」と称す。）を各々格納するフィールドと、任意の情報を送るためのペイロードとが含まれる。

【0006】 次に、IPパケット704の宛先がグローバルIPアドレス「4.17.168.6」であることを検出したル

ータ703は、IPパケット704を宛先アドレス708を行なうIPパケット705としてインターネット712に転送する。宛先アドレス708においては、IPパケット704のSAフィールド内のプライベートIPアドレス「192.168.1.2」を、ルータ703のインターネット側のグローバルIPアドレス「202.224.159.14」に置換する。この際、ルータ703は、IPパケット704のSA「192.168.1.2」とIPパケット705のDA「4.17.168.6」の値を、図8（b）に示すようなルータ703内部に保持されるNATテーブル713に保存する。

【0007】 実施708の結果、IPパケット705はグローバルIPアドレスのみを含み、インターネット上で転送可能なパケットとなる。そのためIPパケット705は目的のサーバ702に転送され、サーバ702でパケット処理（S710）が行なわれ、元のIPパケット706がルータ703に返送される。パケット処理（S710）においてパケットのSAとDAの値は交換される。

【0008】 ルータ703はIPパケット708を受信すると、NATテーブル713との比較を行なう。比較により、IPパケット706のDAはIPアドレス705のSAと一致することから、ルータ703が送出したパケットに対する応答であることを認識し、その後、宛先アドレス709を行なう。

【0009】 図8の実施709において、ルータ703は、IPパケット706のDAフィールド内のグローバルIPアドレス「202.224.159.14」を、IPパケット708のSAフィールド内のIPアドレス「4.17.168.6」に置き換えてNATテーブル713に保存されていた機器701のIPアドレス「192.168.1.2」に置換し、IPパケット707としてLAN711へ転送する。これによりIPパケット707は機器701に返送され、機器701ではIPパケット704のレスポンスとして受信される。

【0010】 NATテーブル713は通信を行なっている関係で、通信が完了すると破棄される。通信完了の特徴は、TCPパケットの場合はSYNパケットの抽出または通信が行なわれない状態によるタイムアウトにより行なわれ、UDPパケットではタイムアウトにより行なわれ、以上により、LAN上のサーバ702とインターネット上の機器701間で通信が可能となる。

【0011】 以上の様に、NAT機能を持つルータにより、LAN上の機器とインターネット上の機器の通信が可能となる一方、NATの仕組みでは、LAN上の複数の機器が同時にインターネット上の機器と通信を行なうためには、同時に通信する機器と同じ数だけのグローバルIPアドレスをNATルータに割り当てる必要がある。グローバルIPアドレスの枯渇現象がもたらされる。この様な問題を解決するためにNATの機能を拡張した

NAPT機能がある。

[0012] 以下、NAPT機能の仕組みを図9の通信シーケンス図に照って説明する。但し、図8のNAPTと同様の動作については説明を略する。NAPTではIPパケットのIPアドレスの変換のみを行なったが、NAPTにおいてはポートの変換も同時に行なう。すなわち、図9の経路変換808において、NAPTと同様の変換処理に加え、ルータ803が現在使用していないポート番号(ここでは「100」とする。)を選び、IPパケット804のSP(ここでは「1」とする。)の内容に置き換えてIPパケット805に変換する。この際、ルータ803は、IPパケット804のSA「192.168.1.2」とIPパケット805のDA「172.168.6」の値に加え、IPパケット804のSP(1)とそれを置換したルータ803のポート(100)の値をルータ803内部のNAPTテーブル813(図9(b)参照)に保存する。

[0013] ルータ803はIPパケット806を受信すると、受信パケットの内容とテーブル813との比較を行なう。比較の結果、受信したIPパケット806のDAがIPアドレス805のSAと一致し、IPパケット806のDPがIPアドレス805のSPと一致すれば、受信したパケット806がルータ803が送出したパケット805に対する応答であることを認識し、その結果、経路変換809を行なう。経路変換809においてはNAPTの動作に加え、IPパケット806のDP(ここでは「100」)の内容を保存してあったIPパケット804のSP(ここでは「1」)に置き換え、IPパケット807に変換する。これにより、LAN上の機器801とインターネット上のサーバ802間で通信が可能となる。上記のNAPT機能によれば、LAN側から接続の機器が同時に通信する場合でも、機器801からの通信をルータのポート番号により区別することができ、正しくルータ803のグローバルIPアドレスが1つだけあれば、ルータのポートの複数回同時に通信を行なうことが可能となる。

[0014] 以上の様に、NAPTまたはNAPT技術によれば、プライベートIPアドレスを持つLAN内の機器からインターネット上のサーバに接続することは容易に可能である。一方で、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望む時に自由に接続することが容易でなく、このため例えば、携帯電話からインターネット経由で、車庫内の家庭用機器に接続して制御するような機能の実現は難しかった。これは、LAN内の機器がプライベートIPアドレスを持つ上、インターネット上の機器からはプライベートIPアドレス宛てにパケットを送出することができないためである。この様な問題を解決するために例えば静的NAPTまたはポートフォワーディングと呼ばれる機能がある。

[0015] 静的NAPT機能においては、ユーザは予めルータに静的NAPTテーブルを設定する必要がある。静的NAPTテーブルのエントリは、接続したいLAN内の機器のIPアドレスとポート、及びルータの任意の空いているポートからなる。ユーザはインターネットからLAN内の機器に接続したい場合は、ユーザの端末から、ルータのグローバルIPアドレスと静的NAPTテーブルに設定されたポートの値を指定してパケット送信を行なう。ルータは、ユーザの端末から受信したパケットの内容を、予め設定してあった静的NAPTテーブルのエントリと照合して、パケットの送信先をエントリ内のLAN内の機器のIPアドレスとポートに置換して転送する。

[0016]

[説明が解決しようとする課題] 以上の静的NAPTにより、インターネット上の機器からLAN内の機器に対し通信が可能になる。しかし、静的NAPTには、予めユーザが静的NAPTテーブルを設定しておく必要がある。その設定内容がIPアドレスの知識のないエンドユーザにとって複雑であるという問題があった。また、ルータのグローバルIPがPPPやDHCPプロトコルにより動的に割り振られている場合に、そのIPアドレスをユーザが把握することが難しく、接続先を特定できないという課題があった。さらに、外部からのパケットをLAN内に転送するためにセキュリティが低下すること、ユーザの管理するルータがISPのプライベートIPアドレスのネットワークに接続されている場合などNAPTが複数行なわれている場合にはISPのルータの静的NAPT設定を行なわなければインターネットから通信が行えないといった、多くの課題があった。

[0017] 以上説明した様に、プライベートIPアドレスを持つLAN内の機器からインターネット上の機器に接続することは容易だが、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望む時に自由に接続することが容易でなかった。このため例えば、PC(パーソナルコンピュータ)や携帯電話からインターネット経由で、車庫内のPCや家庭用機器に接続して制御するような機能の実現は難しかった。

[0018] 本発明は上記の課題を解決することを目的とする。すなわち、本発明はプライベートIPアドレスを持つLAN内の機器に対しインターネット上の機器から望む時に自由に通信できる方法を提供する。特に、その場合に、ユーザがルータに対して事前に接続先を設定を行なう必要がなく、また、ルータのインターネット側IPアドレスが動的に割り振られている場合でも容易に通信先機器を指定でき、またNAPTルータが多数の場合でも、前述の通信を実現できる方法を提供する。

[0019]

[課題を解決するための手段] 本発明に係る第1の通信システムは、インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1

13

つの端末との間の通信を、インターネットに接続されたサーバを介して転送する通信システムである。その通信システムにおいてサーバ及び機器は次のように動作する。

【0020】機器はサーバに定期的な通知パケットを送り、サーバは端末から機器に対する転送要求があった場合、通知パケットの応答として接続要求パケットを機器に送る。機器は、サーバから接続要求パケットを受信した場合、サーバに対してTCP接続要求を返信する。サーバは、接続要求パケットに応じて機器からサーバへ送信されたTCP接続要求を受信し、これによりTCP接続を確立する。サーバは、TCP接続確立後、そのTCP接続上で端末と機器との通信を転送する。

【0021】第1の通信システムによれば、サーバから機器に送信される接続要求パケットは機器からの通知パケットの応答として送信されるため、機器がNAT機能を搭載したルータによってインターネットに接続されている場合でも、接続要求パケットを静的NAT設定無しにルータを通して機器に届けようことができる。またTCP接続の確立に際して機器からサーバに対して接続要求が行われるため、やはり静的NAT設定を無しにTCP接続を確立することが出来る。これによりサーバと機器の間で何時でも恒久的にTCP接続を確立することができ、このTCP接続上でサーバが通信の転送を行うことにより、端末からNATルータの有無に関わらず何時でも恒久的にLANに接続された機器と通信を行うことが可能となる。さらに本発明は、通信の転送を行わない間は負荷の軽いパケットを用い、通信の転送を行う期間は通信の信頼性が高いTCP接続を用いるため、サーバの負荷を軽減しながら信頼性ある通信を実現することができる。

【0022】本発明に係る第2の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。端末はサーバに対し機器IDを含んだHTTPリクエストを送信することにより機器に対する転送要求を行う。サーバは端末と機器との通信を転送する際に、端末からのHTTPリクエストを機器から受取れたTCP接続上に転送する。機器は転送されたHTTPリクエストに対し、それに対するHTTPレスポンスをTCP接続上でサーバへ応答する。サーバはHTTPレスポンスを端末へ転送する。第2の通信システムによれば、既存のWebブラウザを装備した端末から、NATルータの有無に関わらず何時でも恒久的にLANに接続された機器とHTTPによる通信を行うことが可能となる。

【0023】上記の第2の通信システムにおいて、機器はWebサーバモジュールと転送モジュールを備えてもよい。Webサーバモジュールは、転送モジュールからHTTPリクエストを受信してHTTPレスポンスを送信する。転送モジュールは、サーバから接続要求パケットを受信した際はサーバに対してTCP接続要求を送信

(7)

14

してTCP接続を確立し、そのTCP接続上でサーバからHTTPリクエストを受信してWebサーバに転送し、WebサーバからHTTPレスポンスを受信してサーバへTCP接続上で転送する。

【0024】これによれば、既存のWebブラウザを装備した端末から、NATルータの有無に関わらず何時でも恒久的にLANに接続された機器とHTTPによる通信を行うことが可能となるうえ、既存のWebサーバモジュールを機器に実装することができる。

【0025】本発明に係る第3の通信システムは、第1の通信システムにおいてサーバ等が次のように動作する。

【0026】サーバは、少なくとも1つの端末から複数の転送要求を受信することができ、端末から機器に対する複数の転送要求があった場合に、各々一意なセッション識別子を生成し、接続要求パケットにより機器に通知する。機器は、サーバからセッション識別子を持った接続要求パケットを受信した場合、サーバに対してTCP接続を確立し、その確立したTCP接続上でセッション識別子をサーバに送信し、TCP接続確立後、そのTCP接続上でサーバと通信する。サーバは、接続要求パケットに応じて機器からサーバへ送信されたTCP接続要求を受信してTCP接続を確立し、TCP接続上で機器から送信されるセッション識別子を受信し、TCP接続に受信されたセッション識別子を対応付けることで、端末からの複数の転送要求に対して複数のTCP接続を各々対応付ける。サーバは、端末がセッション識別子を指定して接続を要求し、且つ、指定されたセッション識別子に対応付けられたTCP接続が確立済みの場合、確立済みのTCP接続上で端末からの通信を転送することにより、セッション識別子毎に並列して通信内容の転送を行う。

【0027】第3の通信システムによれば、サーバと機器との間に複数のTCP接続を確立することができ、その際の個々のTCP接続上の通信内容を別々のセッションIDで管理することで、内容を混合して一意性を保つことなく、端末から機器に対しセッションID毎に並列した通信を行うことが可能となる。

【0028】第1の通信システムにおいてサーバは複数の機器に対し、機器毎に最終アクセス時刻を記録する記憶手段を備え、次のように動作してもよい。サーバは、機器からの定期的な通知パケットを受信したときに、最終アクセス時刻と通知パケット上の受信時刻とを照合する。そして、端末から機器に対する転送要求があった際に、機器の最終アクセス時刻と現在時刻との差が所定値を超えた場合は、接続要求を拒否する。その差が所定値以下の場合は、通知パケットの応答として接続要求パケットを機器に送る。

【0029】これによれば、機器が動作して通信可能なことが端末からサーバに接続要求があった際に直ちに真

50

図であるため、通信不可能な場合に端末に対する応答の応答が迅速に出来、また機器のIPアドレスがISPによって自動的に割り当てられており、かつ機器の電源断などにより、サーバに登録された機器のIPアドレスが既に同アドレスの機器に割り当てられた場合でも、誤って同アドレスの機器に接続要求を行うことを回避できる。

【0030】本発明に係る第4の通信システムは、図1の通信システムにおいてサーバ等が次のように動作する。

【0031】サーバは、複数の機器に対し、機器毎に最終アクセス時間を記録する記録手段を備える。サーバは、機器による最大アクセス履歴期間情報を送信する。機器は、その最大アクセス履歴期間情報を受信して内部に保存しておき、最大アクセス履歴期間情報が示す期間よりも短い間隔で定期的に通知パケットを送信する。サーバは、機器から通知パケットを受信した際に最終アクセス時間を通知パケットの受信時刻で更新する。サーバは、端末から機器に対する接続要求があった際に、機器の最終アクセス時間と現在時刻との差が最大アクセス履歴期間情報で示す期間を超えている場合は接続要求を拒否し、その差が最大アクセス履歴期間情報で示す期間以下の場合は、通知パケットの応答として接続要求パケットを前記機器に送信する。

【0032】第4の通信システムによれば、機器が動作して通信可能なことが端末からサーバに接続要求があった際に直ちに確認できるため、通信不可能な場合に端末に対する応答の応答が迅速に出来、また機器のIPアドレスがISPによって自動的に割り当てられており、かつ機器の電源断などにより、サーバに登録された機器のIPアドレスが既に同アドレスの機器に割り当てられた場合でも、誤って同アドレスの機器に接続要求を行うことを回避できる。さらに、サーバから機器に予め最大アクセス履歴期間情報を指定することで機器が通信可能な状態であることを確認する通知パケットの送信間隔を制御し、サーバにおいて通知パケットの受信間隔と通信不可能となるまでの時間をトレードオフによって自由に調整することが可能となる。

【0033】本発明に係る第5の通信システムは、図1の通信システムにおいてサーバ等が次のように動作する。

【0034】サーバは、サーバ証明書を持ち、通信を暗号化および復号化する暗号通信手段を備える。端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段とを備える。機器は、通信を暗号化および復号化する暗号通信手段を備える。サーバは、端末と機器の間で秘密情報を転送する際、予め端末にサーバ証明書を送信する。端末は、サーバと秘密情報の送受信を、サーバ証明書を照会して正規であることを確認した後に暗号通信手段により暗号化して行う。機器

は、サーバと秘密情報の送受信を、確立されたTCP接続で暗号通信手段により暗号化して行う。サーバは、確立されたTCP接続を介して端末から機器へ秘密情報を転送する際は、端末から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して機器に送信する。または、機器により確立されたTCP接続を介して機器から端末へ秘密情報を転送する際は、機器から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して前記端末に送信する。

【0035】第5の通信システムによれば、端末と機器の間で秘密に通信を行うことが出来、さらに端末から接続先を認証するためのサーバ証明書が各機器に不要でサーバに1種類で良いと特に効果がある。

【0036】本発明に係る第6の通信システムは、図1の通信システムにおいてサーバ等が次のように動作する。

【0037】サーバは、サーバ証明書を保持し、通信を暗号化および復号化する暗号通信手段を備える。端末は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備える。機器は、サーバ証明書を検証する手段と通信を暗号化および復号化する暗号通信手段を備える。サーバは、端末と機器の間で秘密情報を転送する際、予め前記端末と前記機器に各々サーバ証明書を送信する。端末は、サーバと秘密情報の送受信を、サーバ証明書を照会して正規であることを確認した後に暗号通信手段により暗号化して行う。機器は、サーバと秘密情報の送受信を、サーバ証明書を照会して正規であることを確認した後に機器に確立されたTCP接続上暗号通信手段により暗号化して行う。サーバは、機器により確立されたTCP接続を介して機器から機器へ秘密情報を転送する際は、端末から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して機器に送信する。又は、機器により確立されたTCP接続を介して機器から端末へ秘密情報を転送する際は、機器から暗号化された秘密情報を受信して暗号通信手段で復号化した後、暗号通信手段で暗号化して前記端末に送信する。

【0038】第6の通信システムによれば、端末と機器の間で秘密に通信を行うことができ、さらに端末から接続先を認証するためのサーバ証明書が各機器に不要でサーバに1種類で良いと特に効果がある。

【0039】本発明に係る第7の通信システムは、インターネットに接続された少なくとも1つの機器と、インターネットに接続可能な少なくとも1つの端末との間の通信を、インターネットに接続されたサーバが転送する通信システムである。その通信システムにおいてサーバ等が次のように動作する。

特許3445986

37

【0040】サーバは、複数の機器に対し、機器毎に最終アクセス時刻を記録する記憶手段を備える。機器は、サーバに第1及び第2の通知パケットを定期的に送り、第1の通知パケットの送信間隔は第2の通知パケットの送信間隔よりも長い。サーバは、機器から第1及び第2の通知パケットを受信し、機器から第1の通知パケットを受信したときに最終アクセス時刻を受信時刻で更新し、第2の通知パケットを受信したときには最終アクセス時刻を更新しない。サーバは、端末から機器に対する転送要求があった際に、機器の最終アクセス時刻と現在時刻との差が所定期間を超えている場合は接続要求を拒否し、その差が所定期間以下の場合は、第1及び第2の通知パケットの成否として接続要求パケットを前記機器に送る。機器は、サーバから接続要求パケットを受信した場合、サーバに対してTCP接続要求を送信する。サーバは、接続要求パケットに成否として機器からサーバへ送還されたTCP接続要求を受信し、これによりTCP接続を確立する。サーバは、TCP接続が確立後、そのTCP接続上で端末と機器間の通信を転送する。

【0041】第7の通信システムによれば、機器が動作して通信可能なことが端末からサーバに接続要求があったにもかかわらず到達できないため、通信不可能な場合に端末に対する拒否の応答が高速に出来、また機器のIPアドレスがIPによって自動的に割り当てられており、かつ機器の電源断などにより、サーバに記録された機器のIPアドレスが現在関係無い別の機器に割り当てられた場合でも、誤って関係の無い別の機器に接続要求を行うことを回避できる。さらに本発明によれば、通知パケットを第1および第2の通知パケットの2種類に区別し、最終アクセス時刻更新を第1の通知パケット受信時に限ることで、NATルータが接続要求パケットを通知パケットの応答とみなす時間が短いために通知パケットの送信頻度を高くしなればならない場合でも、サーバにとって負荷の低い最終アクセス時刻更新の頻度を高くなくとも良い結果がある。

【0042】上記の通信システムにおけるサーバ、機器の機能は、コンピュータのようなプログラム可能な装置で所定のプログラムを実行させることにより実現されてもよい。そのプログラムはコンピュータ読み取り可能な記録媒体により提供されてもよい。

【0043】**【発明の実施の形態】**以下、添付の図面を参照し、本発明に係る通信システムの実施の形態を詳細に説明する。
【0044】**（実施の形態1）**図1は本発明の実施の形態1の通信システムの通信シーケンスを説明した図である。図2は本発明の通信システムのネットワーク構成図である。本発明の通信システムはローカルエリアネットワーク（LAN）106上の機器とインターネット105上の機器間の通信を実現するものであり、LAN106に接続された機器101と、インターネット105上

(9)

18

に接続されたサーバ104と、LAN106とインターネットを接続するルータ103とを含む。インターネット105には通信端末102も接続されている。

【0045】ルータ103はNAPT機能を実装している。機器101のIPアドレスはプライベートIPアドレス「192.168.1.2」であり、サーバ104のIPアドレスはグローバルIPアドレス「4.17.168.6」であるとする。ルータ103のインターネット105側アドレスは一般にインターネットサービスプロバイダからDHCPやPPP等のプロトコルにより割り当てられ、動的に変化するが、この時点でルータ103のインターネット側アドレスはグローバルIPアドレス「202.224.159.14」であるとする。説明の便宜上、ルータ103のインターネット105側アドレスは1つしかないとする。なお、本実施の形態において、IPアドレスはIPv4で展開している。

【0046】図1を参照し、本実施形態の通信シーケンスを説明する。機器101はまず、サーバ104に対し最大アクセス確定期間接続要求107を送信する。サーバ104はこの応答として、最大アクセス確定期間接続通知108を送信する。これらの通信107、108はUDPによってもTCPによっても良く、LAN106側に接続された機器101から開始されるため、NAPT機能を備えたルータ103を越えて支障なく通信できる。ここで、最大アクセス確定期間とは、機器101からサーバ104へ送信される通知UDPパケット（後述）の送信時間間隔の最大値を示すものであり、例えば「5分」というような値となる。

【0047】次に、機器101は定期的に通知UDPパケット109を送信する。この間隔は先に説明した最大アクセス確定期間の値（例えば5分）より小さい間隔で送られる。通知UDPパケット109は機器101に固有の付与された機器識別子である「機器ID」を含む。通知UDPパケット109はルータ103により、往路のNAPT変換が行なわれた後インターネット105に送出され、サーバ104にて受信される。

【0048】図3の（a）、（b）に各々変換される前後の通知UDPパケットの内容を示す。通知UDPパケットの送信間隔は、ルータ103がUDPパケットのNAPTテーブルをタイムアウトにより破棄する時間よりも短く設定する。これによりルータ103には、図9（b）に示したようなNAPTテーブルがタイムアウトせず継続的に保持される。

【0049】図1に戻り、サーバ104は、通知UDPパケット109を受信すると、ヘッダ内のSA、DA、SP、DPの名アドレスと機器IDを取り出し、図4に示すように、これらの情報で機器ID1（機器ID＝1234）に対応する1組のエントリとしてサーバ内に登録保持する（ステップS118）。また、ステップS119では、最終アクセス時刻をエントリに付加し、

50

(10)

特許3445986

19

サーバ104が通知UDPパケット109を受信した時刻を記録する。以後、サーバ104は、通知UDPパケット109を受信するたびにステップS120に示すように機器に対応するエントリの最終アクセス時刻を更新する。また、この際、通知UDPパケット109のヘッダ内のSA、SPの各アドレスが変更されている場合は、エントリ中のそれぞれのアドレスの値も更新する。これにより、ルータ103のインターネット(WAN)105側IPアドレスが動的に割り振られていても、最新のアドレスがエントリに保持される。以上のシーケンスの実行により、通信の準備が完了する。

[0050]以上の通信準備が完了している状態で、端末102から機器101に対する通信を開始したい場合、端末102は機器101の機器IDをパラメータに指定して、サーバ104に対し機器接続要求110を送信する。なお、機器IDは端末102が予め記憶しているものとする。機器接続要求110を受信したサーバ104は、端末102により指定された機器IDを検査キーとして図4に示すテーブルからサーバ内に登録された機器IDを検索し、機器101が登録した対応エントリを得る(ステップS121)。

[0051]次に、サーバ104はエントリ内の最終アクセス時刻を参照し、現在時刻との差が最大アクセス確認期間を越えている場合は機器接続要求110を拒否し、最大アクセス確認期間以下の場合は、ステップS122以降に進んで機器101に接続要求UDPパケット111を送信する。

[0052]このように最終アクセス時刻を確認することで、機器101が正常に動作し、かつ、ごく最近まで正常に通信できていたか否かが直ちに確認できるため、機器接続要求110の承諾可否判定が迅速にできる。また、ルータ103のインターネット(WAN)105側IPアドレスはISPによって動的に割り当てられているため、機器101の最終アクセス後何秒間隔で経過すると、サーバ104に登録された機器101のIPアドレスが別の機器に割り当てられてしまう場合があるが、この場合でも照って照合の際に別の機器に接続要求を行うことを防止できる。

[0053]次に、サーバ104は、一意なセッション識別子を生成してサーバ内に保存する(ステップS122)。さらに、サーバ104は機器101に宛てたエントリからSA、DA、SP、DPの各アドレスを取得し、これらを用いてセッション識別子をペイロードを含む接続要求UDPパケット111を送信する。ここで、接続要求UDPパケット111は通知UDPパケット109に対する応答として構成されている。図3(c)にインターネット(WAN)105上を通過された接続要求UDPパケットの内容を示す。図3(c)に示すパケットのアドレスとポートの値は、それぞれ図3(b)に示すパケットにおいてアドレスとポートのソースとディ

20

スティネーションの値を入れ替えた値となっている。これにより、接続要求UDPパケット111は通知UDPパケット109の応答パケットであることが分かる。接続要求UDPパケット111は、ルータ103において経路のNAPT変換により図3(c)に示す構成から図3(d)に示す構成に変換され、機器101に転送される。

[0054]接続要求UDPパケット111を受信した機器101は、サーバ104に対してTCP接続要求112を送信する。TCP接続要求112についての詳細な説明は省略するが、syn, ack/syn, ackパケットによって接続を確立する通常のTCP接続確立手順である。TCP接続要求112はLAN側からWAN側に対して行なわれるものであるため、NAPT機能を含んだルータ103を越えて支障なくTCP接続を確立することができる。

[0055]以上によりサーバ104と機器101の間でTCP接続が確立されたため、UDPパケットはセッションレス型であるため、そのままでサーバ104において、TCP接続が接続要求UDPパケット111に依って確立されたか否かの判定ができなく、そのため以下で説明する手順が実行される。

[0056]まず、機器101はそのTCP接続上で、接続要求UDPパケット111により通知されたセッション識別子を、セッション識別子通知113によってサーバへ返送する。サーバ104はセッション識別子を受信すると、ステップS123においてセッション識別子の照合を行う。照合の結果、このセッション識別子が機器接続要求110により生成されたものであることを検出すると、サーバ104はこのTCP接続と、接続要求110に答えて端末102と機器101間の通信の転送に使用することを決定する。

[0057]なお、セッション識別子に代えて機器IDを用いてもTCP接続と接続要求UDPパケットを対応付けることはできるが、その場合はサーバ104と機器101の間には同時に複数のTCP接続を確立することができるという問題が生じる。本実施形態によれば、サーバ104と機器101の間には複数のTCP接続を確立することができ、その際の個々のTCP接続上の通信内容を別々のセッション識別子で管理することで、複数の通信の内容を混雑せずに混合してしまわずに、別々のTCP接続上で各々一貫性を持った通信の転送を行ない、端末102から機器101に対しセッション識別子値を並列して複数の通信を行うことが可能となる。

[0058]以上述べた手順により、サーバ104と機器101の間でTCP接続が確立されると、サーバ104はそのTCP接続上で端末102と機器101間の通信の転送を開始する。すなわち、サーバ104は端末102からの通信114を通信115として機器101に

(11)

特許3445986

21

伝送し、機器101からの通信116を端末102に通信117として転送する。最後に、通信が完了すると、サーバ104または機器101からTCP切断118を行い、通常のTCP接続の切断を行って一連のシーケンスが完了する。

[0060] なお、上記のサーバ104による通信の伝送は、TCP接続が維持されている間は何度でも繰り返して行なうことが可能であり、これにより端末102と機器101の間で一連の通信を行なうことができる。また、図1では端末104からの通信に対し機器101が応答する様子を示しているが、これに限らず、どの様な手順のプロトコルの通信の伝送をもTCP接続が維持されている間に行なうことが可能である。

[0060] 以上説明したように本実施の形態によれば、通知UDPパケット109への応答として接続要求UDPパケット111を送ることで、プライベートIPアドレスを持つLAN内の機器101に対し、インターネット上の端末102から所望のタイミングで自由に通信を開始できる。これにより、例えば、端末としてインターネットに接続された携帯電話やPDAを用い、機器としてLANに接続される、ビデオ、テレビ、エアコン、冷蔵庫などの家電を用いれば宅外から自由に家電操作を行なうことも可能となる。

[0061] また、本実施の形態によれば、ルータ103は通常のNAPT動作のみを行えばよく、静的NAPT、静的NAPT設定等が不要なため、事前にユーザがルータに対して設定を行なう必要が無い。

[0062] また、本実施の形態によれば、ルータ103に静的NAPTを設定せず、機器101に対してWAN側から到達可能なパケットが、機器101が通知UDPパケットを送信している期間にサーバ104から通信されるパケットに限定される。これにより、第三者からの攻撃を受けにくく、セキュリティが向上する。

[0063] また、本実施の形態によれば、LAN内からインターネットに対して間断的に通知UDPパケット109が送信される。これにより、このパケットがルータ103に対し、いわゆるキープアライブパケットとして作動し、ルータ103のWAN側側のPPPやDHCPがタイムアウトすることによってISPから切断されようとするのを防ぎ、いつでもインターネットから通信可能な状態に維持するという効果を持つ。

[0064] また、本実施の形態によれば、サーバ104から最大アクセス数超過期間経過後108によって通知UDPパケット108の送信間隔の短延を変更することで、サーバにおける通知UDPパケット109の受信負荷と通信不能などの発生を抑えることが可能となる。

[0065] また、本実施の形態によれば、ルータ103のWAN側IPアドレスが動的に割り振られていて、通知UDPパケット108により周期的に最新のWAN

22

AN側IPアドレスがサーバ104に登録されるため、端末102からは機器IDを指定するのみで容易に機器101を指定して通信ができる。

[0066] また、本実施の形態において、負荷の高いUDP通信により通信の遅延を行ない、端末102と機器101との通信自体はデータロスなく信頼性の高いTCP通信を行なうことが好ましい。これにより、サーバ104の負荷の低減と、端末102と機器101との通信の信頼性を両立することができる。通信を要する通知UDPパケット109は、ルータ103のNAPTテーブルのタイムアウト以下の間隔で送出する必要がある。送信頻度が高くなるため、UDPパケットとすることによる負荷削減効果が大きく、一方で周期的に送信されるために多少のパケットロスがあっても次の送信で回復するために影響が小さいなど、UDPパケットを使用する事に特に利点がある。

[0067] なお、本実施の形態ではNAPTによって割り振られた、ルータ103がNAPT動作を行なっている場合であっても、機器101とサーバ104の間作を要するごとに、図1のシーケンスが実行される。また、本実施の形態において、ユーザがNAPT動作を要するルータを用いず、機器101を直接インターネット105に接続している場合であっても、図1のルータ103の動作を変更することなしに、図1のシーケンスが可能となる。さらに、本実施の形態において、ユーザがプライベートIPアドレスを使用するISPに加入し、その結果、ユーザのルータとISPのルータをあわせて多段のNAPTルータを介してインターネットによって接続されている場合でも、その各々の段のルータにおいて通常のNAPTまたはNAPT動作が行なわれ、やはり機器101とサーバ104の間作を変更することなしに、図1のシーケンスが実行される動作する。

[0068] なお、アドレス登録は通知UDPパケットに必要な機能ではなく、他の手段によってアドレス登録を行なっても本発明の効果は失われぬが、周期的な送信が必要な、グローバルIPアドレスを登録するパケットとNAPTテーブルを維持するパケットの2種類を使用するため効率が良く、特に好適な構成である。

[0069] なお、セッション識別子はTCP接続を識別し112に対しTCP接続を一意に識別付与される範囲で一意であれば良く、例えばサーバ内で一意でなくとも、機器IDと組み合わせれば一意であっても良い。

[0070] なお、本実施の形態ではIPverのアドレスを示して説明したが、IPverのアドレスを用いない場合でも、LAN内からインターネットのパケットとこのパケットに対する応答は送達しないルータやゲートウェイを使用する限りにおいて本発明は同じ効果を有する。

[0071] なお、本実施の形態では端末102はイン

(32)

特許3445988

23

ネットワークに直接接続されるように図示されているが、端末102がLANに接続されている端末102から通信を開始する際においてサーバ104に対する通信に支障はないため、本発明の態様は同様に実施される。さらに、端末102に機器101と同様の機能を搭載すれば、端末102と機器101がともにLAN内にある場合にも互いに通信を開始することが出来る構成となり、完全に双方向通信システムを構成できることは明らかである。

【0072】なお、本実施形態では機器101からの接続先はサーバ104のみであり、サーバ104が端末102と機器101間の通信を伝送したが、接続要求UDPパケット111により端末102のアドレスを通知すれば、機器101が端末102に対し直接TCP接続要求112を通信する構成も可能である。この構成によれば、端末102と機器101が通信伝送を行うことが可能となり、サーバ104の伝送負荷が低減されるなど別の効果がある。

【0073】なお、本実施形態においてサーバは端末と機器の通信の転送のみを行ったが、同時にサーバ自身がTCPの接続を用いて機器と通信を行うことも可能である。このように構成すればサーバは端末に対して機器への通信機能を提供すると同時に、機器の設定や監視、ソフトウェアのアップデートを行うなど機器へのサービスを提供することも可能である。

【0074】なお、本実施形態において機器101およびサーバ104をコンピュータで構成することができる。その際に、機器101とサーバ104に各々図1のシーケンスを実行させるコンピュータプログラムを作成することが可能であり、またそれらを各々媒体に記録し配布することができ、これによれば汎用のコンピュータを用いて本発明の通信を実現することができ、

【0075】(実施形態2) 本発明に係る通信システムの別の実施形態を説明する。本実施形態のネットワーク接続は図2で示したとおりである。アドレス付番号1の装置の形態と同じであり、通信シーケンスのみが異なる。本実施形態では端末としてWebブラウザを備えたPCや携帯電話機を用いて、これを用いてLANに接続された機器101とHTTPによる通信を行って動作やコンテンツ取得などを行うものである。

【0076】図5を参照し、本実施形態の通信シーケンスを説明する。機器101はまず、サーバ104に対し最大アクセス制限時間要求407を送信する。サーバ104はこの応答として、最大アクセス制限時間情報通知408を返信し、最大アクセス制限時間の値(例えば5分)を通知する。この通信はUDPによってもTCPによってもよく、LAN106側に接続された機器101から開始されるため、NAPT機能を備えたルータ103を通して支障なく通信できる。

24

【0077】次に、機器101は2種類の通知UDPパケットA、B(410、409)を各々周期的に送信する。2種類のパケットA、Bの送信は、通知UDPパケットAが最終アクセス時間を更新する機能を持っているに對し、通知UDPパケットBは最終アクセス時間を更新する機能を付たないことである。その他の点については同じである。

【0078】機器101から通知UDPパケットA(410)を送信する間隔は先に取得した最大アクセス制限の値(例えば5分)より小さい間隔で送られる。一方、通知UDPパケットAまたはBのいずれかを送信する間隔はルータ103がUDPパケットのNAPTテーブルをタイムアウトにより廃棄する時間よりも短く設定する。

【0079】実施形態の1においては通知UDPパケットは1種類しかなかったため、その送信間隔は設定の条件のうち間隔の短いほうにあわせて設定する必要があった。そのため、ルータ103のNAPTテーブルの廃棄時間が短い(例えば30秒)の場合、通知UDPパケットが30秒間隔以下の高頻度で送られる、その際に最終アクセス時間を更新されるため、ルータ103のWAN側のアドレス変更が頻りに発生してエントリの更新作業が行われ、サーバ負荷が増大するという問題があった。本実施形態は、最終アクセス時間の更新間隔を、ルータ103のNAPTテーブルの廃棄時間と同様なく独立に設定することができ、負荷を軽減しやすいという効果を有する。

【0080】通知UDPパケットA、Bは機器101に固有に付与された機器識別子である機器IDを含む。通知UDPパケットA、Bは、ルータ103により仕組のNAPT変換が施されてインターネットに送出され、サーバ104で受信される。NAPT変換の内容は実施形態の1と同様である。また、通知UDPパケットによりルータ103内のNAPTテーブルがタイムアウトせず自動的に保持される点も同じであり、サーバ104内のエントリに、機器101にパケットを送信するためのアドレスが登録される点(ステップS421)。エントリ中の最新アクセス時間の更新(ステップS422)についても本実施形態の1と同様である。ここまでのシーケンスの実行により、通信の準備が完了する。

【0081】以上の準備動作が完了している状態で、端末102から機器101に対する通信を開始する場合、端末102はサーバ104に対し、「GET connect.cgi?ID=1234」のように機器IDの値をパラメータに指定して、HTTPリクエストとして機器接続要求411を送信する。なお、機器ID「1234」は端末102が予め記憶しているものとする。機器接続要求411を受信したサーバ104は、ステップS423において、指定された機器IDをキーにサーバ内に登録された機器IDを検索し、機器101が登録した対応エントリを得

る。
 [0082] 次に、サーバ104はエンタリ内の最終アクセス時刻（図4参照）を確認し、それと現在時刻との差が最大アクセス履歴期間を超えている場合は接続要求411を拒否し、最大アクセス履歴期間内の場合には、ステップS424以後に進んで機器101に接続要求UDPパケット412を送信する。この最終アクセス時刻の確認により、図1の実例の形態と同様に、誤って両側の別の機器に接続要求を行うことを回避できる等の効果がある。

[0083] 次にサーバ104は、ステップS424において一時的セッション識別子を生成してサーバ104内に保持する。さらに、サーバ104は機器101に対応するエンタリからSA、DA、SP、DPの各アドレスを取得し、これらを用いてセッション識別子をペイロードを含む接続要求UDPパケット412を送信する。ここで、接続要求UDPパケット412は通知UDPパケットA（410）または通知UDPパケットB（409）に上する形式とて構成されているため、ルータ103において、既知のNAPT変換が行われて機器101に転送される。

[0084] 接続要求UDPパケット412を受信した機器101は、サーバ104に対してTCP接続要求413を送信する。TCP接続要求413についての詳細な説明は省略するが、syn, ack/syn, ackパケットによって接続を確立する通常のTCP接続確立手順である。TCP接続要求413はLAN側からWAN側に到達して行なわれるものであるため、NAPT機能を持たないルータ103を超えて支障なくTCP接続を確立することができる。

[0085] 以上によりサーバ104と機器101の間でTCP接続が確立された後、機器101はそのTCP接続上で、接続要求UDPパケット412により通知されたセッション識別子を、セッション識別子通知414によってサーバ104へ返送する。サーバ104はセッション識別子を受信すると、ステップS425でセッション識別子の照合を行い、このセッション識別子が機器101により生成されたものであり、従って機器101に対するTCP接続確立が成功したことを検出する。

[0086] その後、サーバ104はHTTPリクエスト411に対する応答としてHTTPレスポンス415を端末102に返送する。このHTTPレスポンス415は、端末102に提示すべきHTMLコンテンツを含んでおり、かつ、このHTMLコンテンツにはセッション識別子“5678”が、例えば“A-Header: control, comSessionID=5678; deviceFunc, callParam=abcd”のリンクやボタンとして埋め込まれている。以上の手順により、端末102には機器101に対応するページ（図6）が表示される。

[0087] 次に、ユーザが表示されたページ内のリンクをクリックすると、“GET control, comSessionID=5678; deviceFunc, callParam=abcd”等のようにセッション識別子を含むHTTPリクエスト418が生成されてサーバ104に送信される。サーバ104はHTTPリクエスト418を受信すると、指定されたcontrol, callが検出し、セッション識別子“5678”を照合する（ステップS426）。照合した結果、セッション識別子“5678”のTCP接続が既に確立済みであることを検出すると、サーバ104のcontrol, callは、HTTPリクエスト418の内容を“GET deviceFunc, callParam=abcd”のように変換してHTTPリクエスト転送417としてそのTCP接続上に転送する。このようにして、端末102は、機器101に対するHTTPリクエストを送信できる。

[0088] 本発明の端末と機器間の通信経路において、上記で説明したような変換方式を用いると、端末は従来のWebブラウザをなら変換することなく動作可能な上、機器上の“deviceFunc, com”等の所定のcallと“Param=abcd”等の所定のパラメータを指定して始まるHTML文書を機器が自由に返送することが可能となるなど、優れた効果を持つ。

[0089] HTTPリクエスト転送417を受信した機器101は、その応答としてHTTPレスポンス418を送信する。この動作について図8を用いて詳細に説明する。

[0090] 図8に示すように、機器101は転送モジュール501とWebサーバモジュール502を備える。転送モジュール501はサーバ104との間で各種の通信プロトコルによる通信を行なうためのモジュールであり、Webサーバモジュール502は通常のWebサーバである。転送モジュール501は前述の様に、接続要求UDPパケット412を受信してTCP接続要求413を行い、HTTPリクエスト転送417を受信する。この際の転送モジュール501の通信方向に注目すると、TCP接続要求（413）する一方でHTTPリクエスト（417）を受信しており、クライアントからTCP接続を要求され且つHTTPリクエストを受信する通常のWebサーバとは逆逆の方向が異なる。本実施の形態では、転送モジュール501がこの方向の違いを吸収し、Webサーバモジュール502に対し、ソケット等を通して内部的にHTTPリクエスト503の送信、HTTPレスポンス504の受信を行なうことで、通常のWebサーバを用いて、本発明のHTTP通信手順が実現できるという効果を有する。

[0091] 図8に示すように、サーバ104により、HTTPレスポンス418がHTTPレスポンス転送419として端末102に返送される。HTTPレスポンス転送419に含まれるHTMLコンテンツには、セッション識別子がリンクやボタンとして埋め込まれてお

り、手順416~419と同様の手順を繰り返すことにより、端末102から機器101に対して継続的にHTTPによるアクセスを行うことが可能になる。この通信のHTTPメッセージ生成は機器101で行なわれ、コンテンツ表示と操作は端末102で行なわれることにより、端末102から機器101を自由に操作したり、コンテンツを取得したりできる。

[0092] 最後に、通信が完了すると、サーバ104または機器101がTCP切断420を行い、TCP接続の切断を行って一連のシーケンスが完了する。

[0093] 以上説明したように本実施の形態によれば、第1の実施の形態同様、プライベートIPアドレスを持つLAN内の機器101に対し、インターネット上の端末102から任意のタイミングで自由に通信を開始できる。これにより、端末としてWebブラウザを搭載したPCや携帯電話により、家庭内の機器を自由に操作したり、コンテンツを取得することができる。

[0094] また、第1の実施の形態同様、ルータ103は通常のNAT動作のみを行えばよく、静的NAT/NAPT設定等が不要なため、事例にユーザールータに対して複雑な設定を行う必要が無い。

[0095] また、第1の実施の形態同様、第3番からの攻撃を受けにくく、セキュリティが向上するという効果を有する。

[0096] また、第1の実施の形態同様、ルータ103のWAN側接続のPPPやDHCPがタイムアウトすることによってISPから切断されてしまうことを防ぎ、いつでもインターネットから通信可能な状態に維持するという効果を有する。

[0097] また、第1の実施の形態同様、サーバ104における通知UDPパケット4110の受信処理と通信不可能なことを検出するまでの時間を、互いにトレードオフして自由に調整することが可能となる。

[0098] さらに、最終アクセス時刻を変更する機能を持つパケットと持たないパケットの2種類の通知UDPパケットを用意することで、上記の時間の調整も、ルータ103のNATテーブルの検索時間と同様なく確立に行なうことができるという効果を有する。

[0099] また、第1の実施の形態同様、端末102からは機器101を指定するのみで容易に機器101を指定して通信ができる。

[0100] また、第1の実施の形態同様、UDPパケットによるサーバ104の負荷の低さと、TCPパケットによる端末102と機器101との通信の信頼性を両立することができる。

[0101] また、本実施の形態によれば、端末102に通常のWebブラウザを搭載した端末を用い、機器101に通常のWebサーバを搭載してHTTPの応答を実行することができるため、汎用性が高く、ユーザーの使い慣れた通信システムを低コストに構築できる。

[0102] なお、本実施の形態ではNATによって説明したが、ルータ103がNATを行っていない場合であっても、機器101とサーバ104の動作を変更することなしに、図5に示す通信シーケンスを支援無く実現できる。また、本実施の形態において、ユーザーがNATルータを用いず、機器101を直接インターネット105に接続している場合であっても、機器101とサーバ104の動作を変更することなしに、図5のシーケンスが支援無く実現できる。さらに、本実施の形態において、ユーザーがプライベートIPアドレスを使用するISPに加入し、その結果、ユーザーのルータとISPのルータをあわせて多数のNATルータを介してインターネットによって接続されている場合でも、その各々の段のルータにおいて通常のNATまたはNAPT動作が行なわれ、やはり機器101とサーバ104の動作を変更することなしに、図5のシーケンスを支援無く実現できる。

[0103] なお、アドレス登録は通知UDPパケットに必要な情報ではなく、他の手段によってアドレス登録を行なっても本発明の効果は失われず、図5の図示の送信が必要なく、グローバルIPアドレスを登録するパケットとNATテーブルを維持するパケットの2種類の送信のため効率が高く、特に好適な構成である。

[0104] なお、セッション識別はHTTPリクエスト4111に対しTCP接続を一意に対応付けられる範囲で一意であればよく、例えばサーバ内で一意でなくとも、機器101と組み合わせた場合に一意であっても良い。

[0105] また、IPアドレスにIPv6のアドレスを用いてもよい。この場合、LAN内からインターネットへのパケットとそのパケットに対する応答は送信するが、インターネットからLAN内へのパケットは送信しないというクライアント側で使用する限りにおいて本発明は同じ効果を有する。

[0106] なお、本実施の形態では端末102はインターネットに直接接続されるように図示されているが、端末102がLANに接続されている場合でも端末102から通信を開始する限りにおいてサーバ104に対する通信に支障はないため、本発明の効果は同様に発現される。さらに、端末102は機器101と同様の機能を搭載すれば、端末102と機器101がともにLAN内にあっても互いに通信を開始することが出来た構成となり、完全に分離した通信システムを構成できることは明らかである。

[0107] なお、本実施の形態では機器101からの接続先はサーバ104のみであり、サーバ104が端末102と機器101間の通信を転送したが、接続要求UDPパケット412により端末102のアドレスを通知すれば、機器101が端末102に対し直接TCP接続要求413を送信する構成も可能である。この構成に依れば、端末102と機器101が直接通信を行なうこと

が可能になり、サーバ104の転送負荷が低減されるなど別の効果がある。

[0108] なお、本実施の形態においてサーバ104は端末と機器の通信の転送のみを行ったが、同時にサーバ自身がTCP接続を用いた機器と通信を行うことも可能である。このような構成によればサーバは端末に対して機器への通信経路を提供すると同時に、機器の設定や監視、ソフトウェアのアップデートを行うなど機器へのサービスを提供することも可能である。

[0109] なお、本実施の形態において機器101およびサーバ104をコンピュータで構成することができる。その際に、機器101とサーバ104に各々図4のシーケンスを実行させるコンピュータプログラムを作成することが可能であり、またそれらを各々媒体に蓄積し配布することができ、これによれば汎用のコンピュータを用いて車載内からの通信を実現することができる。

[0110] (実施の形態3) 本発明の通信システムの第3の実施の形態を説明する。本実施の形態のネットワーク構成は図5で示されたとおりである。アドレス付与も前述の実施の形態と同じであり、通信シーケンスのみが異なる。本実施の形態では端末としてWebブラウザを備えたPCや携帯電話を用いており、これを用いてLANに接続された機器101とHTTPによる通信を行って操作やコンテンツ取得などを行なう。

[0111] 図7を参照して、本実施の形態の通信シーケンスを説明する。本実施の形態の通信シーケンスは、通知UDPパケットによって通信接続が行われるまでの手順は、図5で示した実施の形態2のシーケンスと同じである。図7にはそれ以降の手順を示している。

[0112] 端末102から機器101に対する通信を開始したい場合、端末102はサーバ104に対し、SSLでのTCP接続要求607を送信する。これにより通常のSSLの手順に従ってサーバ証明書通知608がサーバ104から端末102に送付されて、ステップ624で認証される。認証が成功すると暗号化通信が可能となる。続いて、第2の実施の形態と同じ手順に従って、接続接続要求608からTCP接続要求611までのシーケンスが実行される。

[0113] [0114] 本実施の形態と異なる第1の点は、機器接続接続要求609が暗号化されていることである。これにより機器接続接続要求609に含まれる機器IDを秘匿する点である。また、第2の異なる点は、ステップ626において乱数が生成されてサーバ内に保存され、さらに接続要求UDPパケット810により機器に通知される点である。

[0114] 次に、機器101がTCP/SSL接続要求611を送信し、サーバ104との間でTCP接続を接続する。これにより通常のSSLの手順に従ってサーバ証明書通知612がサーバ104から機器101に送付されて、認証される(ステップ627)。認証が成

功すると暗号化通信が可能となる。

[0115] 以上によりサーバ104と機器101の間でSSLで暗号化されたTCP接続が確立された後、手順613〜614の転送が行われて端末102ページが表示される。その後、ユーザによるリクエストによりセッション識別子を使った手順615〜618のHTTP通信の転送、及び手順619〜622のHTTP通信の転送が行われる。これらのHTTPの転送の内容自体は実施の形態2と同じである。そのため、実施の形態2と異なる点を説明する。

[0116] 本実施の形態と実施の形態2の間の第1の差異は、通信の暗号化がなくなっていることである。これにより機器IDなどの、機器固有の情報やその他の価値のある情報を秘匿にすることができる。

[0117] 本実施の形態と実施の形態2の間の第2の差異は、セッション識別子通知613において、セッション識別子に加えて、機器証明書と、サーバから接続要求UDPパケット810によって送信された乱数とを可及的に通知される点である。機器証明書は機器101が正当であることを証明するものである。機器証明書はステップ628において提供され、正しい機器である場合のみ接続のステップが実行される。機器証明書が暗号化されて送信できることは、本発明の方式にこのような手順で機器証明書認証を組み合わせた場合に特に有利となる。

[0118] さらに、ステップ628において、セッション識別子通知613の引数の乱数が、ステップ628においてサーバ内に保存された乱数と同じであるかを検証し、同じである場合のみ接続のステップが実行される。これにより、接続要求UDPパケット810が本当にサーバが送信したものかどうかを確実に、クラッカーが接続要求UDPパケット810を偽造した場合でも振動を防ぐことができる。

[0119] また、本発明の構成が単一のサーバを必ず経由する構成であるため、サーバ側(サーバ証明書)において暗号を生成する方式と組み合わせる場合、各機器、各端末に個別に証明書を書きずともサーバに送くだけで、複数の機器と複数の端末が存在して互いに接続しようとするシステムにおいても互いを認識しあうことができる。これによりサーバ証明書側の数を削減して管理を容易化できる。また、機器101とサーバ104間のTCP/SSL通信の方向が機器101側からTCP通信を開始する構成のため、サーバ104側は単一のサーバ証明書を書き入れればよく、特にSSLの適用に好適な構成である。

[0120] なお、HTTPリクエストとHTTPレスポンスの対応に通信内容の秘匿も必要性に応じて暗号化の適用/非適用を変更することも可能で、これにより暗号化による負荷を最適化できる。本実施の形態はこれらの効果を第2の実施の形態に加えて保持する。

[0121]

(16)

特許3445986

31

【発明の効果】以上説明するように本発明では、プライベートIPアドレスを持つLAN内の機器に、インターネット上の機器から望み時に自由に通信できる方法を提供し、その際、事前にユーザがルータに対して複雑な設定を行わなくても良く、さらにルータのインターネット側アドレスが動的に割り振られていても容易に通信先機器を指定でき、またNATルータが多数の場合でも動作する方法を提供する。その際に、UDPパケットによるサーバ負荷の低減と、TCPパケットによる端末と機器との通信の信頼性を両立することができる。

【0122】また、静的NATを行なわないためにNAT第3者からの攻撃を受けにくくセキュリティが高く、サーバの通信負荷の軽減が容易であり、通常のWebブラウザを接続した端末とHTTP通信を採用し、汎用性が高くユーザの使い勝手のよい通信システムを低コストに構成することが可能になると、多くの利便性効果が見られる。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態における通信シーケンスを示した図である。

【図2】 本発明の通信システムにおけるネットワーク構成を示した図である。

【図3】 本発明の通信システムにおける通信パケットの内容を示した図である。

【図4】 本発明の通信システムにおけるサーバ内で登録される、機器ID、SA、DA等のアドレス、最終アクセス時刻を含むエントリを示した図である。

【図5】 本発明の第2の実施の形態における通信シーケンスを示した図である。

【図6】 第2の実施の形態の通信システムにおける機器の構成を示した図である。

【図7】 本発明の第3の実施の形態における通信シーケンスを示した図である。

【図8】 従来のNAT機能を持つルータの通信シーケンスを示した図である。

【図9】 従来のNAT機能を持つルータの通信シーケンスを示した図である。

【符号の説明】

32

* 101 機器
102 端末
103 ルータ
104 サーバ
105 インターネット
106 LAN
107、407 最大アクセス確認周期情報要求
108、408 最大アクセス確認周期情報通知
109、409、410 通知UDPパケット
110、411、609 接続接続要求
111、412、610 接続要求UDPパケット
112、413、611 TCP接続要求
113、414、613 セッション識別子通知
415、614 接続接続応答
416、615 HTTPリクエスト
417、616、620 HTTPリクエスト転送
418、617、621 HTTPレスポンス
419、622 HTTPレスポンス転送
501 低送モジュール

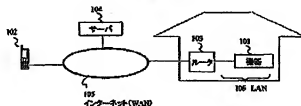
20 502 Webサーバモジュール
612 サーバ側管理通知
613 セッション識別子通知

【要約】

【課題】 LANとインターネット（WAN）が接続されたネットワーク環境においてWAN側の機器からLAN内の機器に所望のタイミングで容易に接続可能とする通信システムを提供する。

【解決手段】 機器101は定期的にサーバ104に対しUDPパケットを送信する。サーバ104は必要な時にこのUDPパケットに対する返信パケットとして通信を送ること、サーバ104から機器101へのNATを施した通信を行なうことができる。特に、サーバ104がまず機器101に対しUDPで接続要求111を送り、機器101はサーバ104からの接続要求111を受け、サーバ104に対してTCP接続112を行う。サーバ104は確立したTCP上で振替電話機等の端末102と機器101間の通信（114-117）を制御する。

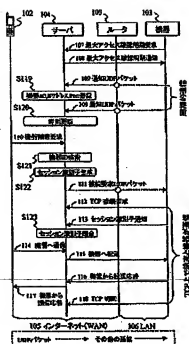
(図2)



(17)

特許3445986

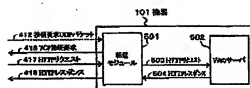
【図1】



【図3】



【図6】



【図4】

項目ID	GA	GA	GP	GP	最終アクセス日時
1234	2008/10/10 10:10	2008/10/10 10:10	100	100	2008/10/10 10:10:00
...

